UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,352	11/13/2001	Art Shelest	212159	8322

22971 7590 09/29/2005

MICROSOFT CORPORATION
ATTN: PATENT GROUP DOCKETING DEPARTMENT
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/010,352	SHELEST ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) *18-20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,21 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

2. Applicant's submission filed on July 11, 2005 has been entered and made of record.

Response to Arguments

3. Applicant's arguments with respect to claims 1 – 17, 20 and 22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1 – 17, 21 and 22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claims 1, 2, 3, 5, 6, 8, 11, 17 and 21 read, " ...usable to route a message to the first computing device...", Claims 3 and 5 read, "...then the public key is discarded.", Claims 6 and 8 read, "the portion of the network address other than the node selectable portion being defined by a network address protocol", Claim 14 reads, "... then discarding the public key and first network address ...", Claim 15 reads, "...then removing from the cache the public key/network address association...." and Claim 16 reads, "...removing the public key/network address...".

With respect to "...usable to route a message to the first computing device...", although the specification discloses the prior art "In protocols typically used today the message contains the network address of the sender (the "from address") and the network of the recipient ("to address").", the specification does not disclose "...usable to

route a message to the first computing device..." (instant application Page 7 paragraph [0029]). The specification does not indicate how the first computing device uses a network address of the first computing device "...usable to route a message to the first computing device..." anywhere in the specification. Applicant amendment does not clarify the steps of "...usable to route a message to the first computing device...".

With respect to "the portion of the network address other than the node selectable portion being defined by a network address protocol", although the specification discloses the prior art "In Ipv6, the node-selectable portion is called "interface identifier" .." (instant application Page 9 paragraph [0033]) and "In steps 704 and 706, the recipient .... recreates the node-selectable portion ...Then the recipient compares the value for the node-selectable portion ...", the specification does not indicate how to compare a portion of a value produced by the hashing with a portion of the network address other than the node-selectable portion, "the portion of the network address other than the node selectable portion being defined by a network address protocol" anywhere in the specification. Applicant remarks/arguments do not address ""the portion of the network address other than the node selectable portion being defined by a network address protocol".

With respect to "... then discarding the public key and first network address ..." and "...then the public key is discarded.", although the specification discloses ".. the recipient discards any message whose public key/address is not in the cache" (instant application Page 4 paragraph [0011]) and "...the recipient compares the identifier in the message with its own identification and discards the message ..."

(instant application Page 12 paragraph [0037]). The specification does not indicate how comparing the first network address ... association already in the cache, then discarding the public key and the first network address" and "...then the public key is discarded.", anywhere in the specification. Applicant amendment does not clarify the steps of "...then discarding the public key and first network address ..." and "...then the public key is discarded.".

With respect to "...then removing from the cache the public key/network address association....", although the specification discloses ".. the recipient discards any message whose public key/address is not in the cache" (instant application Page 4 paragraph [0011]) and "...the recipient compares the identifier in the message with its own identification and discards the message ..." (instant application Page 12 paragraph [0037]). The specification does not indicate how comparing the first network address ... association already in the cache, then removing from the cache the public key/network address association...." anywhere in the specification. Applicant amendment does not clarify the steps o f "...then removing from the cache the public key/network address association....".

The dependent claims 4, 7, 12 – 16 and 22 are rejected at least by virtue of their dependency on the dependent claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 – 17, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie et al (U.S. Patent Number Re. 36,946, hereafter "Diffie") in view of Greg O'Shea (ACM 2000, hereafter "Greg").

6. Regarding Claims 1 and 2, Diffie teaches and describes

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device usable to route a message to the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45); and making the authentication information available to the second computing device, in

part by sending a message to the second computing device, the message including the second digital signature in a packet option and including the network address (Column 6 line 60 – Column 7 line 10 and Column 9 line 46 – Column 10 line 9).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived from the public key of the of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of computing (first) device is derived from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and Integrating CAM into MIPv6").

7. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of two devices. Diffie themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to coming Diffie with O'Shea because security and device authentication is needed for two communicating devices of Diffie and O'Shea provides some details of how to authenticate and secure devices. O'Shea's specialized security system for unilateral authentication protocol could have been modified by Diffie to provide a secure communication link between two devices.

8. Regarding Claims 3 and 5, Diffie teaches and describes

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature, the first network address being usable to route a message to the first computing device; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58);

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data and/or a hash value of data including the content data, wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded (Column 7 line 46 – Column 8 line 58 and Column 12 lines 13 – 36).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived from the public key of the of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of computing (first) device is derived from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and Integrating CAM into MIPv6").

9. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of two devices. Diffie themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to coming Diffie with O'Shea because security and device authentication is needed for two communicating devices of Diffie and O'Shea provides some details of how to authenticate and secure devices. O'Shea's specialized security system for unilateral authentication protocol could have been modified by Diffie to provide a secure communication link between two devices.

10. Regarding Claims 6 and 8, Diffie teaches and describes

hashing the public key; comparing a porting of a value produced by the hashing with a portion of the network address other than the non-selectable portion, the portion of the network address other than the node selectable portion being defined by a network address protocol; if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing, and if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing (Column 5 line 59 – Column 6 line 7; Column 7 lines 6 – Column 8 lines 67; Column 10 lines 41 – 47; and Column 11 lines 58 – 67).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived

from the public key of the of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of computing (first) device is derived from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and Integrating CAM into MIPv6").

11. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of two devices. Diffie themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to coming Diffie with O'Shea because security and device authentication is needed for two communicating devices of Diffie and O'Shea provides some details of how to authenticate and secure devices. O'Shea's specialized security system for unilateral authentication protocol could have been modified by Diffie to provide a secure communication link between two devices.

12. Regarding Claim 9 and 10, Diffie teaches and describes

hashing the public key and at least a portion of the route prefix of the network address, the route prefix being suitable for routing a message to an appropriate link in a network; setting the node-selectable portion of the network address to a portion of the value produced by hashing; checking to see if the network address as set is already in use; and if the network address as set is already in use, choosing a modifier, appending

the modifier to the public key, and repeating the hashing, setting, and checking (Column 5 line 59 – Column 6 line 7; Column 7 lines 6 – Column 8 lines 67; Column 10 lines 41 – 47; and Column 11 lines 58 – 67).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived from the public key of the of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of computing (first) device is derived from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and Integrating CAM into MIPv6").

13. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of two devices. Diffie themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to coming Diffie with O'Shea because security and device authentication is needed for two communicating devices of Diffie and O'Shea provides some details of how to authenticate and secure devices. O'Shea's specialized security system for unilateral authentication protocol could have been modified by Diffie to provide a secure communication link between two devices.

14. Regarding Claims 11 and 17, Diffie teaches and describes

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device usable to route a message to the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58); and

cashing the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data (Column 7 line 38 – Column 10 line 53; Column 11 line 58 - 67 and Column 12 line 13 – 30).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived from the public key of the of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of computing (first) device is derived from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and Integrating CAM into MIPv6").

15. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of two devices. Diffie themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to coming Diffie with O'Shea because security and device authentication is needed for two communicating devices of Diffie and O'Shea provides some details of how to authenticate and secure devices. O'Shea's specialized security system for unilateral authentication protocol could have been modified by Diffie to provide a secure communication link between two devices.

16. Regarding Claim 21, Diffie teaches and describes

a first data field containing data representing a public key of a computing device; and a second data field containing data representing a network address of the computing device the network address being derived at least in part from a hash of the public key and being usable to route a message to the first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53).

Diffie does not explicitly teach that the authentication information includes a network address of the computing device, the network address having a portion derived from the public key of the of the computing device. However, Greg discloses a unilateral authentication protocol wherein a network address of computing (first) device is derived

from the public key of the computing device (Greg Page 2 – 4; "The CAM Protocol", "Home Address Option" and Integrating CAM into MIPv6").

17. Motivation to combine the invention of Diffie with O'Shea's teachings comes from the need for secure transaction and authentication of two devices. Diffie themselves provide a discussion of the need for authentication security but are silent as to the specific details of the technical network address manipulation involved, see Diffie Column 4 line 10 – Column 5 line 33 and Column 6 line 60 – Column 8 line 67. It would have been obvious to one of ordinary skill in the art to coming Diffie with O'Shea because security and device authentication is needed for two communicating devices of Diffie and O'Shea provides some details of how to authenticate and secure devices. O'Shea's specialized security system for unilateral authentication protocol could have been modified by Diffie to provide a secure communication link between two devices.

18. Claim 4 is rejected as applied about in rejecting Claim 3. Furthermore, Diffie teaches and describes wherein the second computing device accesses the public key of the first computing device over an insecure channel to a device in the set: the first computing device and/or a key publishing device (Column 7 lines 38 – 55).

19. Claim 7 is rejected as applied about in rejecting Claim 6. Furthermore, Diffie teaches and describes wherein the portion of the address other than the node-

selectable portion comprises an element including a "u" bit, "g" bit, and/or a portion of a route prefix (Column 5 line 59 – Column 6 line 25).

20. Claim 12 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address (Column 7 line 41 – Column 8 line 11).

21. Claim 13 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information (Column 3 lines 45 – 52).

22. Claim 14 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes comparing the first network address against a network address in a public key/network address in a public key/network address association already in the cache; and if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then discarding the public key and the first network address without caching them (Column 7 line 38 – Column 10 line 47).

23. Claim 16 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes associating a timer with the caching of the public key/network address association; resetting the timer if a second public key/network address association, identical to the public key/network address association, is presented for caching; and if the timer expires, removing the public key/network address association from the cache (Column 7 line 38 – Column 10 line 47).

24. Claim 22 is rejected as applied about in rejecting Claim 21. Furthermore, Diffie teaches and describes a third data field containing data representing a time stamp (Column 7 line 7 – 10).

25. Claim 15 is rejected as applied about in rejecting Claim 14. Furthermore, Diffie teaches and describes if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then removing from the cache the public key/network address association already in the cache (Column 10 lines 41 – 52).

Conclusion

26. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892. Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz

Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
September 25, 2005.

Primary Examiner
AU 2131
9/27/05